UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,503	04/24/2001	Richard Alan Dayan	RPS9 2001 0011	5669

53493	7590	10/25/2006	

LENOVO (US) IP Law
Mail Stop ZHHA/B675/PO Box 12195
3039 Cornwallis Road
. RTP, NC 27709-2195

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/841,503	DAYAN ET AL.
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *08 August 2006*.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *37-62* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *37-62* is/are rejected.
7) ☒ Claim(s) *38-49 and 51-62* is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *08 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1   This action is in response to the communication filed on 8/8/2006.

2   **DETAILED ACTION**

3   *Continued Examination Under 37 CFR 1.114*

4   A request for continued examination under 37 CFR 1.114, including the fee set forth in

5   37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

6   eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

7   has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

8   37 CFR 1.114. Applicant's submission filed on 8/8/2006 has been entered.

9   *Response to Arguments*

10   Applicants' arguments filed 8/8/2006 have been fully considered but they are not

11   persuasive. Applicants argues primarily that:

12   a.   Gafken teaches away from storing the BIOS in a hard drive.

13   b.   Hayashi does not teach individual verification of the source of each entry.

14   Regarding applicants' argument a., that Gafken teaches away from storing the BIOS in a

15   hard drive, the examiner does not find the argument persuasive. First, Gafken teaches that the

16   specific embodiment disclosed is not meant to be limiting and the updating procedure can be

17   applied to different data and different storage mediums, as can be seen in Col. 14 Paragraph 6.

18   Furthermore, simply because Gafken did not specifically disclose storing the BIOS in the hard

19   drive, does not mean he is teaching away from the combination, but rather shows that in the

20   preferred embodiment of Gafken the BIOS is stored in flash memory. As such, the examiner

21   contends that a *prima facie* case of obviousness has been established and therefore has

22   maintained the rejection.

1   In response to applicants' argument b., that the references fail to show certain features of

2   applicant's invention, it is noted that the features upon which applicant relies (i.e., individual

3   verification of the source of each entry) are not recited in the rejected claim(s). Although the

4   claims are interpreted in light of the specification, limitations from the specification are not read

5   into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6   Rather, the claim simply requires that the source of each entry be verified. The signature

7   verification of Gafken, which verifies the source of the entire upgrade through digital signatures

8   as can be seen in Col. 12 Paragraph 7 – Col. 13 Paragraph 1, meets these limitations and as such

9   the examiner does not find the argument persuasive.

10   All rejections and objections not specifically set forth below have been withdrawn.

11   Claims 37-62 have been examined, and claims 1-36 have been cancelled.

12   *Claim Objections*

13   Claims 38-49 and 51-62 are objected to because of the following informalities: The

14   limitation "the protected partition is found match a portion" in claims 38 and 51 is not

15   grammatically correct. The examiner suggests changing the claim to recite "the protected

16   partition is found to match a portion" in order to be grammatically correct. Appropriate

17   correction is required.

18

19   *Claim Rejections - 35 USC § 103*

20   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

21   obviousness rejections set forth in this Office action:

22   *A patent may not be obtained though the invention is not identically disclosed or described as set forth*
23   *in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art*
24   *are such that the subject matter as a whole would have been obvious at the time the invention was made to a*

1   *person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived*
2   *by the manner in which the invention was made.*
3
4   Claims 37, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken

5   (US Patent Number 6,026,016), further in view of Arnold et al. (US Patent Number 5,128,995)

6   hereinafter referred to as Arnold, and further in view of Menezes et al. ("Handbook of Applied

7   Cryptography") hereinafter referred to as Menezes.

8   Regarding claim 37, Gafken disclosed a method for providing a capability to securely

9   update information stored in a plurality of computer systems (See Gafken Fig. 5), where in the

10   method comprises: forming a protected partition within each of the computer systems (See

11   Gafken Col. 4 Paragraphs 3-4); storing within nonvolatile storage (See Gafken Fig. 1 Element

12   118) of each computer system in the plurality of computer systems, an operating system (See

13   Gafken Fig. 1 Element 150), and an initialization routine (See Gafken Fig. 1 Element 151) to

14   execute within a processor of the computer system after power on of the computer system (See

15   Gafken Col. 3 Paragraph 2 Lines 1-4), wherein the initialization routine includes instructions

16   causing the protected partition to be locked before the operating system is loaded (See Gafken

17   Col. 13 Paragraph 9 – Col. 14 Paragraph 2), and wherein instructions causing information stored

18   within a predetermined location to be written within the protected partition after predetermined

19   security procedures have occurred but before the protected partition is locked (See Gafken Col.

20   13 Paragraph 8); establishing a network connecting each computer system in the plurality of

21   computer systems with a server system (See Gafken Col. 3 Paragraph 6 and Col. 12 Paragraph

22   7); generating an update partition file within the server system (See Gafken Col. 12 Paragraph 7

23   – Col. 13 Paragraph 1); transmitting the update partition file over the network to each computer

24   system in the plurality of computer systems (See Gafken Col. 12 Paragraph 7); and storing the

1   update partition file within the predetermined location of each computer system in the plurality

2   of computer systems (See Gafken Col. 12 Paragraph 5), however, Gafken failed to disclose the

3   protected partition being within a hard drive, or a setup password stored in the nonvolatile

4   storage for use in the predetermined security procedures. However, Gafken did disclosed that

5   "although the example...describes a flash memory used to store...a BIOS...other types of

6   nonvolatile memories storing other types of information may be used" (See Gafken Col. 14

7   Paragraph 6).

8   Arnold teaches that a BIOS can be stored in a protected partition of a hard drive (See

9   Arnold Col. 2 Line 63 – Col. 3 Line 12).

10   It would have been obvious to the ordinary person skilled in the art at the time of

11   invention to employ the teachings of Arnold in the BIOS updating system of Gafken by storing

12   the BIOS in a protected partition of a hard drive instead of flash memory. This would have been

13   obvious because the ordinary person skilled in the art would have been motivated to provide a

14   fast and efficient way to store BIOS code.

15   Menezes teaches that providing a sequence number (password), stored and updated at

16   both a receiver and a sender, in a digital signature of the sender, protects the signature against

17   replay attacks (See Menezes Page 399 Section (ii)).

18   It would have been obvious to the ordinary person skilled in the art at the time of

19   invention to employ the teachings of Menezes to the validation signatures of Gafken by

20   providing a sequence number in the signature of the update image. This would have been

21   obvious because the ordinary person skilled in the art would have been motivated to provide

22   protection against illicitly signed updates.

1   Regarding claim 50, Gafken disclosed an interconnected system for providing

2   updated information in a secure manner (See Gafken Abstract and Fig. 5), wherein the

3   interconnected system comprises: a network (See Gafken Col. 3 Paragraph 6 and Col. 12

4   Paragraph 7); a server system connected to the network and programmed to generate an update

5   partition file and to transmit the update partition file over the network (See Gafken Col. 12

6   Paragraph 7 – Col. 13 Paragraph 1); a computer system connected to the network, wherein the

7   computer system includes a processor (See Gafken Fig. 1), non-volatile data storage including a

8   protected partition (See Gafken Fig. 1 Element 115 and Col. 4 Paragraphs 3-4), wherein the

9   processor is programmed to receive the update partition file from the network and to store the

10   update partition file in a predetermined location within the nonvolatile data storage outside the

11   protected partition (See Gafken Col. 12 Paragraphs 5-7), and wherein the nonvolatile data

12   storage stores an operating system and an initialization routine executing within the processor

13   after power on of the computer system (See Gafken Fig. 1 Element 118 and Col. 3 Paragraph 2

14   Lines 1-4), including instructions causing the protected partition to be locked before the

15   operating system is loaded (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 2), and

16   instructions causing information stored within the predetermined location to be written within the

17   protected partition after predetermined security procedures have occurred but before the

18   protected partition is locked (See Gafken Col. 13 Paragraph 8), but Gafken failed to disclose the

19   protected partition being within a hard drive, or a setup password stored in the nonvolatile

20   storage for use in the predetermined security procedures. However, Gafken did disclosed that

21   "although the example…describes a flash memory used to store…a BIOS…other types of

1   nonvolatile memories storing other types of information may be used" (See Gafken Col. 14

2   Paragraph 6).

3   Arnold teaches that a BIOS can be stored in a protected partition of a hard drive (See

4   Arnold Col. 2 Line 63 – Col. 3 Line 12).

5   It would have been obvious to the ordinary person skilled in the art at the time of

6   invention to employ the teachings of Arnold in the BIOS updating system of Gafken by storing

7   the BIOS in a protected partition of a hard drive instead of flash memory. This would have been

8   obvious because the ordinary person skilled in the art would have been motivated to provide a

9   fast and efficient way to store BIOS code.

10   Menezes teaches that providing a sequence number (password), stored and updated at

11   both a receiver and a sender, in a digital signature of the sender, protects the signature against

12   replay attacks (See Menezes Page 399 Section (ii)).

13   It would have been obvious to the ordinary person skilled in the art at the time of invention to

14   employ the teachings of Menezes to the validation signatures of Gafken by providing a sequence

15   number in the signature of the update image. This would have been obvious because the

16   ordinary person skilled in the art would have been motivated to provide protection against

17   illicitly signed updates.

18

19   Claim 38-43 and 51-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over

20   the combination of Gafken, Arnold, and Menezes as applied to claims 37 and 50 above, and

21   further in view of Hasbun et al. (U.S. Patent Number 6,088,759) hereinafter referred to as

22   Hasbun.

1   Regarding claims 38 and 51, the combination of Gafken, Arnold, and Menezes disclosed

2   after determining that said update partition is stored within said computing system for updating

3   said protected partition, writing a portion of said update partition file to said protected partition

4   (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further

5   modification of information stored within said protected partition (See Gafken Col. 13 Paragraph

6   9 – Col. 14 Paragraph 1), but failed to disclose overwriting similar parts and appending new

7   parts.

8   Hasbun teaches that a bios update can be allocated into virtual blocks so that the blocks

9   can be updated individually without having to erase the entire memory first (See Hasbun Col. 5

10   Paragraph 6 – Col. 6 Paragraph 2 and Col. 12 Line 59 – Col. 16 Line 27). Hasbun also teaches

11   that new blocks should be allocated from existing free memory (See Hasbun Col. 7 Paragraph 2).

12   It would have been obvious to the ordinary person skilled in the art at the time of

13   invention to employ the teachings of Hasbun to the bios updating system of Gafken, Arnold, and

14   Menezes by updating each update part one at a time. This would have been obvious because the

15   ordinary person skilled in the art would have been motivated to provide a safe method for

16   updating a bios without risking loss of the entire bios in the event of a power failure.

17   Regarding claims 39 and 52, the combination of Gafken, Arnold, Menezes, and Hasbun

18   disclosed that a flag bit is set in non-volatile storage within said computing system when said

19   update partition file is stored at a predetermined location in non-volatile storage within said

20   computing system (See Gafken Col. 13 Paragraphs 3-4), and determining whether said update

21   partition is stored within said computing system for updating said protected partition is

1   performed by determining whether said flag bit is set (See Gafken Col. 13 Paragraph 7 and Fig. 5

2   Step 550).

3   Regarding claims 40 and 53, the combination of Gafken, Arnold, Menezes, and Hasbun

4   disclosed that after determining that said update partition file is stored within said computing

5   system for updating said protected partition, verifying whether said update partition file has been

6   generated by a trusted server system, and said portion of said update partition is written to said

7   protected partition only following verification that said update partition file has been generated

8   by a trusted server system (See Gafken Col. 12 Paragraph 6 – Col. 13 Paragraph 1 and Figure 6).

9   Regarding claims 41 and 54, the combination of Gafken, Arnold, Menezes, and Hasbun

10   disclosed that verification that said update partition file has been generated by said trusted server

11   system includes: forming a first message digest by applying a hash algorithm to a portion of said

12   update partition file; forming a second message digest by decrypting a digital signature within

13   said update partition file using a public key of said trusted server system; and determining that

14   said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 –

15   Col. 13 Line 2).

16   Regarding claims 42 and 55, the combination of Gafken, Arnold, Menezes, and Hasbun

17   disclosed the predetermined setup procedures include verifying that said update partition file has

18   been generated by said trusted server system includes signing an encrypted portion of said update

19   partition file with a public key of said trusted server system, and said encrypted portion of said

20   update partition file has been prepared by signing, with a private key of said trusted server

21   system, a result of the application of an algorithm to data including a version of said setup

1   password accessed by said trusted server system (See the rejection of claim 37 above and Col. 12

2   Paragraph 7 – Col. 13 Paragraph 1).

3   Regarding claims 43 and 56, the combination of Gafken, Arnold, Menezes, and Hasbun

4   disclosed that the data includes said version of said setup password appended to a portion of said

5   update partition file (See rejection of claim 5 above), said algorithm is a hash algorithm

6   generating a message digest (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), and

7   verifying that said update partition file has been generated by said trusted server system includes

8   applying said hash algorithm to said setup password stored within said computing system

9   appended to a portion of said update partition file to generate a first version of a message digest

10   and comparing said first version of said message digest with a second version of said message

11   digest obtained by signing said encrypted portion of said update partition file (See Gafken Col.

12   12 Paragraph 7 – Col. 13 Paragraph 1).

13   Claims 44-48 and 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over

14   the combination of Gafken, Arnold, Menezes, and Hasbun as applied to claims 38 and 51 above,

15   and further in view of Hayashi et al. (US 2001/0039651 A1) hereinafter referred to as Hayashi.

16   Regarding claims 44 and 57, the combination of Gafken, Arnold, Menezes, and Hasbun

17   disclosed digitally signing the update file and verifying the signature prior to updating the

18   partition (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but the combination of

19   Gafken, Arnold, Menezes, and Hasbun failed to disclose encrypting portions of the file

20   separately and verifying each portion individually.

21   Hayashi teaches a method for providing a variety of software safely by breaking the file

22   into pieces and decrypting each piece separately (See Hayashi Page 1 Col. 2 Paragraphs 3-10).

1   It would have been obvious to the ordinary person skilled in the art at the time of

2   invention to employ the teachings of Hayashi to the updating system of the combination of

3   Gafken, Arnold, Menezes, and Hasbun by encrypting parts of the file separately from the other

4   parts. This would have been obvious because the ordinary person skilled in the art would have

5   been motivated to provide users with customized software without imposing too much of a load

6   on the provider. In this combination, it would also be obvious that each block contained

7   information to be stored in a different location from the other blocks. This would have been

8   obvious because the ordinary person skilled in the art would have been motivated not perform

9   unnecessary computation during the update.

10   Regarding claims 45 and 58, the combination of Gafken, Arnold, Menezes, Hasbun, and

11   Hayashi disclosed forming a first message digest by applying a hash algorithm to said entry, and

12   forming a second message digest by signing said encrypted element associated with said entry

13   using a public key of said trusted server system, and determining that said first and second

14   message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

15   Regarding claims 48 and 61, the combination of Gafken, Arnold, Menezes, Hasbun, and

16   Hayashi disclosed that information stored in said protected partition is compared to each entry in

17   said plurality of entries within said update partition, when a matching portion of said information

18   stored in said protected partition is found to be similar to said entry, said matching portion is

19   overwritten with said entry if space around said matching portion is sufficient, and when a

20   matching portion of said information stored in said protected partition is not found to be similar

21   to said entry, said entry is appended to said information stored in said protected partition if space

22   within said protected partition is sufficient (See the rejection of claim 38 above).

1   Regarding claims 46-47 and 59-60, see the rejection of claims 42-43 above.

2

3   Claims 49 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over the

4 combination of Gafken, Arnold, Menezes and Hasbun as applied to claim 1 above, and further in

5 view of Schmidt (U.S. Patent Number 5,826,015).

6   The combination of Gafken, Arnold, Menezes and Hasbun disclosed a secure bios

7 updating system (See rejection of claim 38 above) but failed to disclose requiring a user to input

8 a password to unlock the bios write capabilities. However, Gafken, Arnold, Menezes and

9 Hasbun did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13

10 Paragraph 1).

11   Schmidt teaches that in order to remotely upgrade a bios, an administrator password

12 should be provided in order to unlock the partition (See Schmidt Fig. 9 and abstract).

13   It would have been obvious to the ordinary person skilled in the art at the time of

14 invention to employ the teachings of Schmidt to the bios updating system of Gafken, Arnold,

15 Menezes and Hasbun by requiring a correct password to be entered in order to unlock the bios

16 altering capabilities. This would have been obvious because the ordinary person skilled in the art

17 would have been motivated to protect the current bios from accidental or illicit alterations.

18   *Conclusion*

19   Claims 37-62 have been rejected, and claims 1-36 have been cancelled.

20   The prior art made of record and not relied upon is considered pertinent to applicant's

21 disclosure.

1   i.   Harmer (US Patent Number 5,835,760) disclosed a system which stores a

2   BIOS in a Hard Drive and searches for portions in the BIOS to update.

3   ii.   Zinger et al. (US Patent Number 6,836,847) disclosed that a Hard Drive

4   could be used in place of Flash Memory.

5   iii.   Jakubowski et al. (US Patent Number 7,080,249) disclosed verification of

6   code blocks.

7   iv.   Pitzel et al. (US Patent Number 7,062,765) disclosed individual

8   downloading and verification of components.

9

10   Any inquiry concerning this communication or earlier communications from the

11 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

12 The examiner can normally be reached on M-F 8-4.

13   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

14 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

15 organization where this application or proceeding is assigned is 571-273-8300.

1   Information regarding the status of an application may be obtained from the Patent

2   Application Information Retrieval (PAIR) system. Status information for published applications

3   may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

4   applications is available through Private PAIR only. For more information about the PAIR

5   system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

6   system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

7   like assistance from a USPTO Customer Service Representative or access to the automated

8   information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9
10
11
12
13
14   Matthew Henning
15   Assistant Examiner
16   Art Unit 2131
17   10/16/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100